ROSSBACH LAW, P.C.
William A. Rossbach
401 North Washington Street
P.O. Box 8988
Missoula, MT 59807-8988
Phone: (406) 543-5156
Fax: (406) 728-8878
Email: bill@rossbachlaw.com

CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Tiara Avaness (SBN 343928)
tavaness@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070

Counsel for Plaintiff and the Proposed Classes

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MONTANA

BUTTE DIVISION

JESSIE LEAL, on behalf of herself and all others similarly situated, Plaintiff, v. TICKETMASTER, LLC., SNOWFLAKE, INC., and LIVE NATION ENTERTAINMENT, INC. Defendants.	Case No CV-24-46-BU-BMM **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jessie Gabriela Leal ("**Plaintiff**") individually and on behalf of all others similarly situated, bring this Class Action Complaint (the "**Complaint**"), and allege the following against Defendants Ticketmaster, LLC ("**Ticketmaster**"), Snowflake, Inc. ("**Snowflake**"), and Live Nation Entertainment, Inc. ("**Live Nation**") (collectively, "**Defendants**"), based upon personal knowledge with respect to herself and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Plaintiff's and other similar situated individuals' personal identifiable information ("**PII**"), including but not limited to "full names, addresses, email addresses, phone numbers, ticket sales and event details, order information, and partial payment card data. [The] compromised payment data includes customer names, the last four digits of card numbers, expiration dates, and even customer fraud details" (collectively, "**Private Information**").[1]

2. This class action arises out of the recent targeted cyberattack against Defendant Ticketmaster's Data Cloud virtual warehouse, managed by Defendant

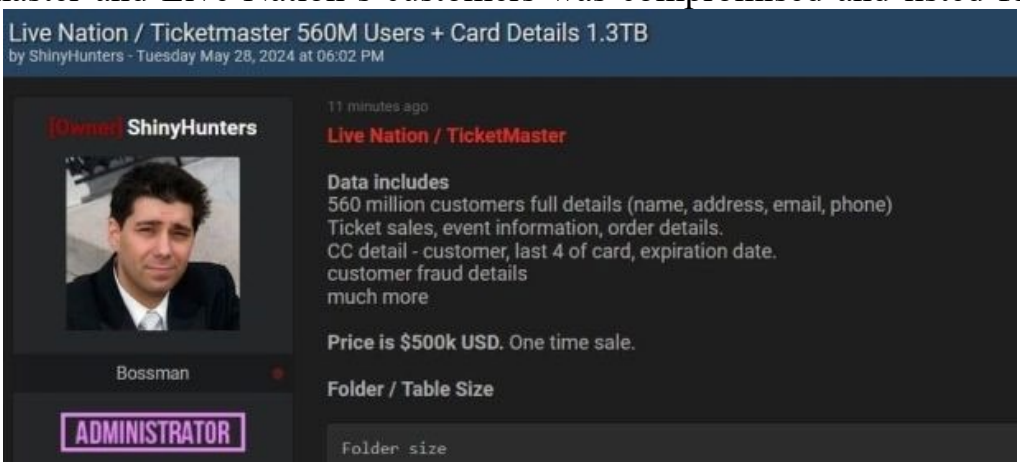
[1] Waqas, *Hackers Claim Ticketmaster Data Breach: 560M Users' Info for Sale at $500k,* HACKREAD (May 29, 2024), https://hackread.com/hackers-ticketmaster-data-breach-560m-users-sale/. (last visited June 12, 2024).

Snowflake, that enabled a third party to access Defendants' computer systems and data, resulting in the compromise of highly sensitive Private Information (the "**Data Breach**").[2]

3. Due to the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their Private Information.

4. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' Private Information.

5. On or around May 28, 2024, the Private Information of 560,000,000 Ticketmaster and Live Nation's customers was compromised and listed for sale.[3]



[2] *Id.*

[3] Georgie Hewson, *Home Affairs Department confirms cyber incident impacting Ticketmaster customers*, ABC NEWS (May 29, 2024),

The notorious hacker group known only by its alias "ShinyHunters" claimed that it had stolen 1.3 terabytes of personal data and is reportedly ready to sell, or has already sold, such information to nefarious dark web users for $500,000, as illustrated by their post on BreachForums, a dark-web marketplace for stolen data:

6. This Data Breach occurred because Defendants collectively enabled an unauthorized third party to gain access to and obtain former and current Ticketmaster and Live Nation's customers' Private Information from Ticketmaster's systems housed by Snowflake.[4]

7. Ticketmaster and Live Nation store customer data in a virtual warehouse provided by Defendant Snowflake, a cloud data warehouse provider offering its "Data Cloud" to institutional customers to consolidate and store data.[5]

8. As stated in their own privacy policy, Ticketmaster/Live Nation recognize the heavy burden of protection and security that they bear when collecting and storing data. Ticketmaster represents and emphasizes the following:

> "We're always taking steps to make sure your information is protected and deleted securely," "[we] have security measure in place to protect your information,"[6] and "[the] security of our fans' information is a

---

https://www.abc.net.au/news/2024-05-29/ticketmaster-hack-allegedlyshinyhunter-customers-data-leaked/103908614. (last visited June 12, 2024).

[4] *Id.*

[5] *Form 10-K Annual Report for Snowflake, Inc.*, BAMSEC, https://www.bamsec.com/filing/164014724000101?cik=1640147 (last visited June 12, 2024).

[6] *Privacy Policy*, TICKETMASTER, https://privacy.ticketmaster.com/privacy-policy (last visited June 12, 2024).

> priority for us. We take all necessary security measures to protect personal information that's shared and stored with us."

9. Customers provide their PII to Ticketmaster with the expectation that the company will take "**all** necessary security measures," and that its would contract with data warehouse providers who shared the belief that the security of customers' PII is "a priority."

10. Defendants' representation of "all necessary security measures" has proven false, misleading, and stands in stark contrast to their purported prioritization of information security—Defendants admittedly failed to safeguard the PII of millions of its customers and failed to implement all necessary measures to prevent information from being stolen.

11. A criminal was able to access Defendants' Data Cloud, and obtained access to the types of information that federal and state law require companies take security measures to protect, including, but not limited to: ***full names, addresses, email addresses, phone numbers, ticket sales and event details, order information, and partial payment card data including customer names, the last four digits of card numbers, expiration dates, and customer fraud details.***

12. Both the hacker group and Ticketmaster have confirmed that the stolen

database was hosted by Snowflake.[7] [8]

13. Plaintiff, and everyone affected, are now victims of identity theft—as any combination of this PII will forever subject them to being targets of cyber-attacks. The private information exfiltrated is highly substantial and will affect the victims of this data breach, Plaintiff and the putative class, forever. Even years from now, Plaintiff and other victims will be subject to cyber-attacks, and phishing scams.

14. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols, consistent with the industry standard, "necessary" to protect Private Information from the foreseeable threat of a cyberattack.

15. Any entity that prioritizes the security of customers' information, employing "all necessary security measures," would ensure that it and all parties it contracts with had secure procedures to access its Data Cloud environment. Defendants did not do so, electing to brazenly utilize the Snowflake Data Cloud product knowing that Ticketmaster/Live Nation administrators could not enforce Multi-Factor Authentication ("**MFA**").

---

[7] Zach Whittaker, *Live Nation Confirms Ticketmaster Was Hacked, Says Personal Information Stolen in Data Breach*, TECHCRUNCH (May 31, 2024), https://techcrunch.com/2024/05/31/live-nation-confirms-ticketmaster-was-hacked-says-personal-information-stolen-in-data-breach. (last visited June 12, 2024).

[8] Roni Lichtman, *Snowstorm Surrounding the Recent Snowflake Hack*, MEDIUM (June 1, 2024), https://medium.com/@ronilichtman/snowstorm-surrounding-the-recent-snowflake-hack-ab7e51e0c5be. (last visited June 12, 2024).

16. MFA is a simple yet robust security system that requires more than one method of authentication from independent categories of credentials (i.e., a username/password and confirmation link sent via email). MFA is "a critical component in protecting against identity theft, and specifically against attacks related to the successful theft of passwords."[9]

17. ShinyHunters boasted to journalists that the Data Breach was enabled by Snowflake's lack of MFA enforcement.[10] Snowflake inexplicably leaves the option to enable MFA up to individual users, so data environments can be compromised through "weak links" – users who elect to not enroll in MFA for their accounts.[11]

18. MFA administrator enforcement is the industry standard, according to Ofer Maor, cofounder and Chief Technology Officer of data security investigation firm Mitiga.[12] He notes that "most SaaS (soft-as-a-service) vendors, once deployed

---

[9] Shane Snider, *Snowflake's Lack of MFA Control Leaves Companies Vulnerable, Experts Say*, INFORMATIONWEEK (June 5, 2024), https://www.informationweek.com/cyber-resilience/snowflake-s-lack-of-mfa-control-leaves-companies-vulnerable-experts-say. (last visited June 12, 2024).

[10] *Id.*

[11] *FAQ: Multi-Factored Authentication (MFA)*, SNOWFLAKE (August 5, 2023), https://community.snowflake.com/s/article/MFA-FAQs. (last visited June 12, 2024).

[12] Solomon Klappholz, *With Hundreds of Snowflake Credentials Published on the Dark Web, It's Time for Enterprises to Get MFA in Order*, ITPRO (June 7, 2024), https://www.itpro.com/security/cyber-attacks/with-hundreds-of-snowflake-credentials-published-on-the-dark-web-its-time-for-enterprises-to-get-mfa-in-order. (last visited June 12, 2024).

as an enterprise solution, allow administrators to enforce MFA… they require every user to enroll in MFA when they first login and make it longer possible for users to work without it." A data security firm's principal simply noted it is "surprising that the built-in account management within Snowflake doesn't have more robust capabilities like the ability to enforce MFA."[13]

19. Any entity employing "all necessary" data security practices and procedures would monitor for a data security breach. In other words, even if a company negligently left the "bank vault" open (as Defendants did for ***eleven days*** following the Data Breach), it would still have videos monitoring the bank vault, and alarms that would go off if intruders tried to leave with the loot. However, Defendants failed to implement many standard monitoring and alerting systems, evinced by Defendant's inaction in the eight days following the data breach. In Live Nation's recent May 31, 2024, filing with the SEC, it ***confirmed*** that the Data Breach occurred on May 20, 2024.

20. Upon information and belief, Ticketmaster and Live Nation were aware of prior data breaches caused by compromised Snowflake environments, yet took no remedial or preemptive measures to ensure that their customers' data was protected (such as, by way of example, implementing a company-wide policy to enable MFA, or requesting that Snowflake employees with access to Ticketmaster's

[13] Snider, *supra* note 9

cloud environment enable MFA).

21. By acquiring Plaintiff's and class members' Private Information for their own pecuniary benefit, Defendants assumed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class Members' Private Information against unauthorized access and disclosure.

22. Ticketmaster and Live Nation chose to host its data on the Snowflake Data Cloud, and IT professionals at Ticketmaster/Live Nation were on notice that they, as administrators of the platform, were unable to enforce MFA systems. Neither Defendant took any actions to ensure the safety of customers' PII, and instead knew that they had designed systems flawed with issues, and it was a matter of time for the systems to be breached. Recklessly, neither Defendant took any action to stop the preventable data breach. Accordingly, each Defendant shirked its duty to protect customers' and employees' information from being accessed by threat actors.

23. Defendants further had a duty to adequately safeguard this Private Information under controlling case law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act (the "**FTC Act**").

24. Defendants breached those duties and disregarded the rights of Plaintiff and the Class Members by intentionally, willfully, recklessly, or negligently failing

to implement proper and reasonable measures to safeguard consumers' Private Information; failing to take available and necessary steps to prevent unauthorized disclosure of data; and failing to follow applicable, required, and proper protocols, policies, and procedures regarding the encryption of data.

25. As a result of Defendants' inadequate security and breach of their duties and obligations, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unauthorized criminal third party. Plaintiff and Class Members have suffered injuries as a direct and proximate result of Defendants' conduct. These injuries include: (i) diminution in value and/or lost value of Private Information, a form of property that Defendants obtained from Plaintiff and Class Members; (ii) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their Private Information; (iii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the continued, long term, and certain increased risk that unauthorized persons will access and abuse Plaintiff's and Class Members' Private Information; (v) the continued and certain increased risk that the Private Information that remains in Defendants' possession is subject to further unauthorized disclosure for so long as Defendants fail to undertake proper measures to protect the Private Information; (v) invasion of privacy and increased risk of fraud and identity theft; and (vi) theft

of their Private Information and the resulting loss of privacy rights in that information. This action seeks to remedy these failings and their consequences. Plaintiff and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they should be entitled to injunctive and other equitable relief.

26. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiff's and Class Members' sensitive and confidential Private Information remains in the possession of Defendants. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft. The aggregate data compromised in the Data Breach, taken as a whole, including but not limited to: full names, addresses, email addresses, phone numbers, ticket sales and event details, order information, and partial payment card data including customer names, the last four digits of card numbers, expiration dates, and customer fraud details, increases the risk of harm, making identity theft a likely outcome.

27. Defendants disregarded the rights of Plaintiff and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Private Information; failing to take standard and reasonably available steps to

prevent the Data Breach; and failing to properly train its staff and employees on proper security measures.

28. In addition, Defendants failed to properly monitor the computer network and systems that housed the Private Information. Had Defendants properly monitored these electronic systems, Defendants would have discovered the intrusion sooner or prevented it altogether.

29. The security of Plaintiff's and Class Members' identities is now at substantial risk because of Defendants' wrongful conduct as the Private Information that Defendants collected and maintained are now in the hands of data thieves. This present risk will continue for the course of their lives.

30. Armed with the Private Information accessed in the Data Breach, data thieves can commit a wide range of crimes.

31. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Further, Plaintiff and Class Members will incur out-of-pocket costs to purchase adequate credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

32. Plaintiff and Class Members will also be forced to expend additional

time to review credit reports and monitor their financial accounts for fraud or identity theft. And because they exposed other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

33. Plaintiff brings this lawsuit on behalf of herself and all those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that they collected and maintained.

34. Plaintiff, on behalf of herself and all other Class Members, bring claims for negligence, negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, and for declaratory and injunctive relief. To remedy these violations of law, Plaintiff and Class Members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendants' data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

JURISDICTION AND VENUE

35. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332 of the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs, and (iii) there is minimal diversity because at least one Plaintiff (CA) and Defendant (MT) are citizens of

different states. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367 Pursuant to 28 U.S.C. Section 1391.

36. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District: Defendant Snowflake is registered in Montana and headquartered in this District, Defendant Snowflake gains revenue and profits from doing business in this District, and Defendant Snowflake employs numerous people in this District.

37. Defendant Snowflake is subject to personal jurisdiction in Montana as a resident of this state. Defendant Snowflake is authorized to do and is doing business, advertises, and solicits business within the state. By residing in Montana, Defendant is physically present and subject to its laws.

38. Defendants Ticketmaster/Live Nation are subject to personal jurisdiction in Montana based on sufficient minimum contacts which exist between Defendants Ticketmaster/Live Nation and Montana, and the decisions affecting consumers data privacy stored on the Snowflake Data Cloud stem from communications between Defendant Ticketmaster and Montana-based Defendant Snowflake. Defendants Ticketmaster/Live Nation advertises and solicits business in Montana and has purposefully availed itself to the protections of Montana law and should reasonably expect to be hauled into court in this District.

PARTIES

Plaintiff Jessie Gabriela Leal

39. Plaintiff Leal is a citizen of the State of California. At all relevant times, Plaintiff has resided in the county of Los Angeles, California.

40. Since at least 2020, Plaintiff Leal has been Defendants' customer and Ticketmaster account holder. Plaintiff provided her Private Information to Defendants, including her credit card. In receiving and maintaining her Private Information for business purposes, Defendants expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff Leal's Private Information. Defendants, however, did not take proper care of Plaintiff Leal's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of Defendants' inadequate cybersecurity measures.

41. Plaintiff Leal is deeply concerned by the Data Breach because she frequently uses Ticketmaster to purchase concert tickets. Plaintiff Leal continues to worry about her Private Information, as it is readily available for cybercriminals to sell, buy, and exchange, on the Dark Web.

42. Since learning about the Data Breach, Plaintiff anticipates needing to spend substantial time to determine the extent and gravity of the Data Breach and to mitigate damages. Plaintiff will need to review for fraudulent activity and closely monitor her financial information.

43. Plaintiff Ryan suffers a substantially increased risk of fraud, identity theft, and data misuse resulting from her Private Information being leaked on to the Dark Web and subjected to unauthorized third parties/criminals.

44. Plaintiff Ryan has a continuing interest in ensuring that her Private Information, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Defendant Snowflake, Inc.

45. Defendant Snowflake, Inc. is a Delaware corporation headquartered in Montana with its principal executive office located at 106 E. Babcock, Suite A Bozeman, MT 59715.

46. Snowflake is a publicly traded corporation listed on the New York Stock Exchange with revenues totaling approximately $829 million for the three months ended on April 30, 2024.[14]

47. Snowflake's Data Cloud platform is used globally, with 9,437 institutions trusting Snowflake to manage and store customers' data.[15]

48. Due to the nature of the services Snowflake provides, it receives and is

[14] *Form 10-Q Quarterly Report for Snowflake, Inc.*, BAMSEC, https://www.bamsec.com/filing/164014724000135?cik=1640147 (last visited June 12, 2024).
[15] *Form 10-K Annual Report for Snowflake, Inc.*, BAMSEC, https://www.bamsec.com/filing/164014724000101?cik=1640147 (last visited June 12, 2024).

entrusted with securely storing consumers' Private Information, which includes, inter alia, individuals' full name, payment information, occasional location data, and other sensitive information. As a contracting party entrusted with millions of customers' PII, Snowflake was expected to provide confidentiality and adequate security for the data it collected in accordance with Defendant Ticketmaster's promises and disclosures and is expected to comply with statutory privacy requirements.

Defendant Ticketmaster, LLC.

49. Defendant Ticketmaster, LLC. is a wholly owned subsidiary of Defendant Live Nation Entertainment, Inc. headquartered in California with its principal executive office located at 9348 Civic Center Drive, Beverly Hills, CA 90210.

50. Ticketmaster and Live Nation Entertainment completed their merger on January 25, 2010.[16]

51. Ticketmaster "operates as a ticket distribution company. [Ticketmaster] buys, transfers, and sells tickets for live music, sporting, arts, theater, and family

[16] *Live Nation and Ticketmaster Entertainment Complete Merger*, SECURITIES AND EXCHANGE COMMISSION (Jan. 25, 2010), https://www.sec.gov/Archives/edgar/data/1335258/000119312510012287/dex991.htm. (last visited June 12, 2024).

events. Ticketmaster serves clients worldwide."[17]

52. Plaintiff and Class Members are current and former customers of Ticketmaster and account holders on Ticketmaster.com.

53. Due to the nature of the services Ticketmaster provides, it receives and is entrusted with securely storing consumers' Private Information, which includes, inter alia, individuals' full name, payment information, occasional location data, and other sensitive information. Ticketmaster promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

Defendant Live Nation Entertainment, Inc.

54. Defendant Live Nation Entertainment, Inc. is a Delaware corporation headquartered in California with its principal executive office located at 9348 Civic Center Drive, Beverly Hills, CA 90210.

55. Live Nation Entertainment is a publicly traded corporation listed on the New York Stock Exchange with revenues totaling approximately $3.8 billion for the

[17] *Ticketmaster LLC*, BLOOMBERG, https://www.bloomberg.com/profile/company/0009574D:US. (last visited June 12, 2024).

three months ended on March 31, 2024.[18]

56. Live Nation is "the largest live entertainment company in the world, connecting over 765 million fans across all of our concerts and ticketing platforms in 49 countries during 2023."[19]

57. Due to the nature of the services Live Nation provides, it receives and is entrusted with securely storing consumers' Private Information, which includes, inter alia, individuals' full name, payment information, occasional location data, and other sensitive information. Live Nation promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

FACTUAL ALLEGATIONS

A. The Data Breach, and Defendants Unsecure Data Management.

58. On May 28, 2024, threat actors posted that 1.4 terabytes of Private Information were available for purchase on the hacking website Breach Forums.[20] The notorious hacking group ShinyHunters offered the trove of Plaintiff's and Class

[18] *Form 10-Q Quarterly Report for Live Nation Entertainment, Inc.*, BAMSEC, https://www.bamsec.com/filing/133525824000071?cik=1335258. (last visited June 12, 2024).
[19] *Form 10-K Annual Report for Live Nation Entertainment, Inc.*, BAMSEC, https://www.bamsec.com/filing/133525824000017?cik=1335258. (last visited June 12, 2024).
[20] Waqas, *supra* note 1.

Members' Private Information for $500,000.

59. Defendants have ***confirmed*** the Data Breach occurred on May 20, 2024, noting there was "unauthorized activity within a third-party cloud database environment."[21] Such data includes, according to the hackers' forum post, "560 million customers [*sic*] full details (name, address, email, phone) – Ticket sales, event information, order details – CC [credit card] detail [*sic*] – customer, last 4 of card, expiration date. Customer fraud details – much more."[22] Defendants waited ***eleven*** days to confirm the breach.

60. Prior to the Data Breach in May 2024, Plaintiff and Class Members had provided their Private Information to Ticketmaster with the reasonable expectation and mutual understanding that Ticketmaster would comply with its obligations to keep such information confidential and secure from unauthorized access. In particular, Plaintiff and Class Members provided their names, emails, phone numbers, location data and credit card information to Ticketmaster in order to register for an account and purchase event tickets on Ticketmaster.com.

---

[21] *Form 8-K Current Report for Live Nation Entertainment, Inc.*, SEC.GOV, https://www.sec.gov/Archives/edgar/data/1335258/000133525824000081/lyv-20240520.htm?=7194ef805fa2d04b0f7e8c9521f97343 (last visited June 12, 2024).
[22] *Id.*

61. PII is a valuable property right.[23] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[24] It is estimated that American companies have spent over $19 billion on acquiring personal data of consumers in 2018.[25] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years. Indeed, the threat actor who compromised Defendants' systems is seeking a one-time payment of half a million dollars in exchange for this Private Information.

62. Plaintiff and the Class's Private Information exposed in the Data Breach has been exposed on the Dark Web.

63. Ticketmaster promised consumers it would keep their data secure and

---

[23] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26-38 (May 2015), https://www.researchgate.net/publication/283668023. (last visited June 12, 2024). The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

[24] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD No. 220 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en. (last visited June 12, 2024).

[25] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/. (last visited June 12, 2024).

private. Data security is purportedly a critical component of Ticketmaster's business model. On a section of its website, Ticketmaster confidently asserts the following statements:

> "We're always taking steps to make sure your information is protected and deleted securely," "[we] have security measure in place to protect your information,"[26] and "[the] security of our fans' information is a priority for us. We take all necessary security measures to protect personal information that's shared and stored with us."[27]

64. On its website, Ticketmaster maintains an "Our Commitments" section, including "Security & Confidentiality" as one of "10 commitments that drive [Ticketmaster's] privacy program, globally".[28]

65. Contrary to Ticketmaster's various express assurances that it would take reasonable measures to safeguard the sensitive information entrusted to it, it chose to host customers' data on the Snowflake Data Cloud, with full knowledge that its administrators could not enforce MFA security systems, and an unauthorized, criminal element was able to access customers' data because of this decision.

66. To date, Ticketmaster has not disclosed complete specifics of the attack, such as whether ransomware has been used.

67. As such, Ticketmaster, and its parent company Live Nation, have failed

---

[26] *Privacy Policy*, TICKETMASTER, https://privacy.ticketmaster.com/privacy-policy (last visited June 12, 2024)..

[27] *Our Commitments*, TICKETMASTER, https://privacy.ticketmaster.com/en/our-commitments (last visited June 12, 2024).

[28] *Id.*

to secure the PII of the individuals that provided their sensitive information. Defendants failed to take appropriate steps to protect the PII of Plaintiff and other Class Members from being disclosed.

B. Defendants Failed to Comply with FTC Guidelines

68. Defendants were prohibited by the Federal Trade Commission Act (the "**FTC Act**") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "**FTC**") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

69. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

70. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their

network's vulnerabilities; and implement policies to correct any security problems.[29] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[30]

71. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

72. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the

---

[29] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (last visited June 12, 2024).

[30] *Id.*

Federal Trade Commission Act ("**FTCA**"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

73. These FTC enforcement actions include actions against healthcare providers and partners like Defendants. *See, e.g.*, In the Matter of Labmd, Inc., A Corp, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

74. Defendants failed to properly implement basic data security practices, allowing for this attack to occur, victimizing millions of people.

75. Defendants' failure to employ reasonable and appropriate measures to protect against

unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

76. Defendants were at all times fully aware of the obligation to protect the Private Information of customers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

C. Plaintiff and the Class Have Suffered Injury as a Result of Defendants' Data Mismanagement

77. As a result of Defendants' failure to implement and follow even the most basic security procedures, Plaintiff and Class Members' Private Information has been and are now in the hands of an unauthorized third-party which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiff and Class Members now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to the Data Breach.

78. Plaintiff and Class Members have had their most personal and sensitive Private Information disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

79. Plaintiff and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim for cybercrimes for years to come.

80. As a result of Private Information's real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This

information from various breaches, including the information exposed in the Data Breach, can be aggregated, and become more valuable to thieves and more damaging to victims.

81. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[31] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[32]

82. Consumers place a high value on the privacy of that data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[33]

83. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus

---

[31] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs//. (last visited June 12, 2024).

[32] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/. (last visited June 12, 2024).

[33] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), accessible at https://www.jstor.org/stable/23015560?seq=1 (last visited June 12, 2024).

deprived that consumer of the full monetary value of the consumer's transaction with the company.

84. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.[34] The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency, State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Defendants on notice, long before the Data Breach, that 1) cybercriminals are targeting large, public companies such as Defendants Live Nation and Snowflake; 2) cybercriminals were ferociously aggressive in their pursuit of large collections of PII like that in possession of Defendants; 3) cybercriminals were selling large volumes of PII and corporate information on Dark Web portals; 4) the threats were increasing.

85. Had Defendants been diligent and responsible, they would have known about and acted upon warnings published in 2017 that 93% of data security breaches were avoidable and the key ***avoidable*** causes for data security incidents are:

a. Lack of complete assessment, including internal, third-party, and cloud-based systems and services;

[34] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), accessible at https://www.law360.com/articles/1220974 (last visited June 12, 2024).

b. Not promptly patching known/public vulnerabilities, and not having a way to process vulnerability reports;

c. Misconfigured devices/servers;

d. Unencrypted data and/or poor encryption key management and safeguarding;

e. Use of end-of-life (and thereby unsupported) devices, operating systems and applications;

f. Employee errors and accidental disclosures — lost data, files, drives, devices, computers, improper disposal;

g. Failure to block malicious email; and

h. Users succumbing to business email compromise (BEC) and social exploits.[35]

86. Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in

[35] Gretel Egan, OTA Report Indicates 93% of Security Breaches Are Preventable, PROOFPOINT (Feb. 7, 2018), available at https://www.proofpoint.com/us/securityawareness/post/ota-report-indicates-93-security-breaches-are-preventable (last visited June 12, 2024).

a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

87. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, because of Defendants' conduct. Further, the value of Plaintiff's and Class Members' Private Information has been diminished by its exposure in the Data Breach.

88. As a result of Defendants' failures, Plaintiff and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their Private Information.

89. Plaintiff and members of the Class suffered actual injury from having Private Information compromised as a result of Defendants' negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their Private Information, a form of property that Defendants obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

90. For the reasons mentioned above, Defendants' conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm.

91. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard Private Information.

92. Plaintiff, individually and on behalf of all other similarly situated individuals, allege claims in negligence, negligence per se, breach of implied contract, unjust enrichment, violations of the California Consumer Privacy Act, California Legal Remedies Act, and California's Unfair Competition Law.

CLASS ACTION ALLEGATIONS

93. Plaintiff brings this action on behalf of themselves and on behalf of all other persons similarly situated ("**the Class**").

94. Plaintiff proposes the following Class and Subclass definitions, subject to amendment(s) as appropriate:

Nationwide Class

> All individuals residing in the United States whose Private Information was compromised as a result of the Data Breach. ("**the Class**").

California Subclass

> All individuals identified by Defendants (or their agents or affiliates) as being those persons residing in California impacted by the Data Breach. (the "**California Subclass**").

95. Collectively, the Class and California Subclass are referred to as the Classes.

96. Excluded from the Classes are Defendants' officers and directors, and any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

97. Plaintiff reserve the right to amend or modify the Class or Subclass definitions as this case progresses.

98. **Numerosity:** Upon information and belief, the members of the Class are so numerous that joinder of all of them is impracticable.

99. **Predominance of Common Questions**. There exist questions of law and fact common to the Class, which predominate over any questions affecting individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendants were subject to (and breached) the FTC Act, and/or the CCPA;

g. Whether Defendants breached their duty to Class Members to safeguard their Private Information

h. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

i. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants' acts breached an implied contract they formed with Plaintiff and the Class Members;

l. Whether Defendants were unjustly enriched to the detriment of Plaintiff and the Class;

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

100. **Typicality:** Plaintiff's claims are typical of those of other Class

Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

101. **Adequacy:** Plaintiff is an adequate representatives for the Class because their interests do not conflict with the interests of the Class that they seek to represent. Plaintiff has retained counsel competent and highly experienced in complex class action litigation counsel intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their experienced counsel.

102. **Superiority:** A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them by Defendants. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an

economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based upon, inter alia, the records (including databases, e-mails, dealership records and files, etc.) Defendants maintain regarding their consumers.

103. Defendants have acted on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

CLAIMS FOR RELIEF

COUNT 1
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

104. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

105. Defendants owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their Private Information in its possession, custody, or control.

106. Defendants knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class Members' Private Information and the importance of maintaining secure systems. Defendants knew, or should have known, of the vast uptick in data breaches in recent years. Defendants had a duty to protect the Private Information of Plaintiff and Class Members.

107. Given the nature of Defendants' business, the sensitivity and value of

the Private Information it maintains, and the resources at its disposal, Defendants should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Defendants had a duty to prevent.

108. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Private Information entrusted to it—including Plaintiff's and Class Members' Private Information.

109. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' Private Information to unauthorized individuals.

110. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and the Class Members, their Private Information would not have been compromised.

111. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well- established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Class)

112. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

113. Defendants' duties arise from Section 5 of the FTC Act ("**FTCA**"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure Private

Information.

114. Defendants violated Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' Private Information and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information it obtains and stores, and the foreseeable consequences of a data breach involving Private Information including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

115. Defendants' violations of Security Rules and Section 5 of the FTCA constitute negligence per se.

116. Plaintiff and Class Members are within the class of persons that Security Rules and Section 5 of the FTCA were intended to protect.

117. The harm occurring because of the Data Breach is the type of harm Security Rules and Section 5 of the FTCA were intended to guard against.

118. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' Private Information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' Private

Information to unauthorized individuals.

119. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendants' violations of Security Rules and Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their Private Information; (iii) breach of the confidentiality of their Private Information; (iv) deprivation of the value of their Private Information, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach; and (vi) actual or attempted fraud.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class)

120. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

121. Plaintiff and Class Members either directly or indirectly gave Defendants their Private Information in confidence, believing that Defendants would protect that information. Plaintiff and Class Members would not have provided Defendants with this information had they known it would not be adequately

protected. Defendants' acceptance and storage of Plaintiff's and Class Members' Private Information created a fiduciary relationship between Defendants and Plaintiff and Class Members. Considering this relationship, Defendants must act primarily for the benefit of their consumers, which includes safeguarding and protecting Plaintiff's and Class Members' Private Information.

122. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. They breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' Private Information, failing to safeguard the Private Information of Plaintiff and Class Members it collected.

123. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their Private Information which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the Private Information

compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

124. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein. This claim is pleaded in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

125. Plaintiff and Class Members conferred a monetary benefit upon Defendants in the form of monies paid for services.

126. Defendants accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendants also benefitted from the receipt of Plaintiff's and Class Members' Private Information.

127. As a result of Defendants' conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

128. Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws

and industry standards.

129. Defendants should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it because of the conduct and Data Breach alleged herein.

COUNT V
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Nationwide Class)

130. Plaintiff realleges and incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

131. Defendants required Plaintiff and Class Members to provide or authorize the transfer of their Private Information for Defendants to provide services. In exchange, Defendants entered implied contracts with Plaintiff and Class Members in which Defendants agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' Private Information and to timely notify them in the event of a data breach.

132. Plaintiff and Class Members would not have provided their Private Information to Defendants had they known that Defendants would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

133. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendants.

134. Defendants breached the implied contracts by failing to safeguard

Plaintiff's and Class Members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

135. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Defendants' breach of its implied contracts with Plaintiff and Class Members.

COUNT VI
VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 Cal. Civ. Code §§ 1798.100 et seq. ("CCPA")
(On Behalf of the California Subclass)

136. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

137. As more personal information about consumers is collected by businesses,

consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access.

138. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

139. Defendants are subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

140. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure because of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

141. Plaintiff is a "consumer" as defined by Civ. Code § 1798.140(g) because they are natural persons residing in the state of California.

142. Defendants are a "business" as defined by Civ. Code § 1798.140(c).

143. The CCPA provides that "personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . . (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." See Civ. Code § 1798.150(a)(1); Civ. Code § 1798.81.5(d)(1)(A).

144. Plaintiff's Private Information compromised in the Data Breach

constitutes "personal information" within the meaning of the CCPA.

145. Through the Data Breach, Plaintiff's private information was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format.

146. The Data Breach occurred because of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

147. Simultaneously herewith, Plaintiff is providing notice to Defendants pursuant to Cal. Civ. Code § 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiff alleges Defendants have violated or are violating. Although a cure is not possible under the circumstances, if (as expected) Defendants are unable to cure or do not cure the violation within 30 days, Plaintiff will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

148. As a result of Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks statutory damages of up to $750 per class member (and no less than $100 per class member), actual damages to the extent they exceed statutory damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT VII
VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT
Cal. Civ. Code §§ 1750 et seq. ("CLRA")
(On Behalf of the California Subclass, against TicketMaster and Live Nation only)

149. Plaintiff realleges and incorporates by reference every allegation contained elsewhere in this Complaint as if fully set forth herein.

150. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "**CLRA**"), California Civil Code § 1750, et seq. This cause of action does not seek monetary damages currently and is limited solely to injunctive relief. Plaintiff will later amend this Complaint to seek damages in accordance with the CLRA after providing Defendants with notice required by California Civil Code § 1782.

151. Plaintiff and Class Members are "consumers," as the term is defined by California Civil Code § 1761(d).

152. Plaintiff, Class Members and Defendants have engaged in "transactions," as that term is defined by California Civil Code § 1761(e) by acquiring services of Ticketmaster and Live Nation for personal and not commercial use.

153. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct undertaken by Defendants was likely to deceive consumers.

154. Cal. Civ. Code § 1770(a)(2) prohibits Live Nation and Ticketmaster from misrepresenting the source, sponsorship, approval or certification of goods or services. Both Defendants violated this provision by making *commitments* and promises to customers and Plaintiff specifically regarding its services, security, and privacy.

155. Cal. Civ. Code § 1770(a)(5) prohibits both Defendants (Live Nation and Ticketmaster) from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have." Here, both Defendants violated this provision by misrepresenting its services as being of specific qualities, approval, and providing benefits – the promised commitments and security of customers' information. Both Defendants sold its services with the representations of security and confidentiality, none of which were truthful.

156. Similarly, Cal. Civ. Code § 1770(a)(7) prohibits both Defendants from representing their goods and services are of a particular standard, quality, or grade. Here, both Defendants misrepresented the standards and quality of their services and products, while knowing that their security, privacy policies, and processes do not meet even the industry standards, contain serious security issues, and put any customer using/purchasing Defendants' goods or services at risk of having customers' confidential information exposed.

157. Both Defendants also violated Cal. Civ. Code § 1770(a)(16) by failing to supply its goods and services in accordance with their previous representations.

158. Ticketmaster and Live Nation violated CLRA provisions by representing that they took appropriate measures to protect Plaintiff's and the Class Members' Private Information Additionally, Ticketmaster and Live Nation improperly handled, stored, or protected either unencrypted or partially encrypted data, utilized Snowflake's services while knowing of critical issues and lack of appropriate security measures in Snowflake's systems. Ticketmaster and Live Nation also failed to instruct Snowflake to implement the necessary security measures to ensure that their customers confidential information remains protected.

159. As a result, Plaintiff and the Class Members were induced to provide their Private Information to Defendants.

160. As a result of engaging in such conduct, Ticketmaster and Live Nation have violated Civil Code § 1770.

161. Plaintiff seeks an order of this Court that includes, but is not limited to, an order enjoining Defendants from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

162. Plaintiff and the Class Members suffered injuries caused by Defendants' misrepresentations, because they provided their Private Information believing that Defendants would adequately protect this information.

163. Plaintiff and Class Members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

164. The unfair and deceptive acts and practices of Defendants, as described above, present a serious threat to Plaintiff and members of the Class.

COUNT VIII
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW Cal. Bus. and Prof. Code §§ 17200, et seq. ("UCL")
(On Behalf of the California Subclass)

165. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

166. Plaintiff brings this claim on behalf of themselves and the California Class.

167. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, et seq. ("**UCL**"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

168. By reason of Defendants' above-described wrongful actions, inaction, and omission, the resulting Data Breach, and the unauthorized disclosure of Plaintiff's and Class Members' Private Information, Defendants engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

169. Defendants' business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive,

unscrupulous, and substantially injurious to consumers, in that the private and confidential Private Information of consumers has been compromised for all to see, use, or otherwise exploit.

170. Defendants' practices were unlawful and in violation of the CCPA and CLRA and Defendants' own privacy policy because Defendants failed to take reasonable measures to protect Plaintiff's and Class Members' Private Information.

171. Defendants' business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the Private Information they provide to Defendants will remain private and secure, when in fact it was not private and secure.

172. Plaintiff and Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Defendants' above-described wrongful actions, inaction, and omissions including, inter alia, the unauthorized release and disclosure of their Private Information.

173. Defendants' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200 et seq., in that Defendants' conduct was substantially injurious to Plaintiff and Class Members, offensive to public policy, immoral, unethical, oppressive, and unscrupulous, and

the gravity of Defendants' conduct outweighs any alleged benefits attributable to such conduct.

174. But for Defendants' misrepresentations and omissions, Plaintiff and Class Members would not have provided their Private Information to Defendants or would have insisted that their Private Information be more securely protected.

175. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information, they have been injured as follows: (1) the loss of the opportunity to control how their Private Information is used; (2) the diminution in the value and/or use of their Private Information entrusted to Defendants; (3) the increased, imminent risk of fraud and identity theft; (4) the compromise, publication, and/or theft of their Private Information; and (5) costs associated with monitoring their Private Information, amongst other things.

176. Plaintiff takes upon herself enforcement of the laws violated by Defendants in connection with the reckless and negligent disclosure of Private Information. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to penalize Plaintiff by forcing her to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

b. For an order granting permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein, including:

   i. Requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

   ii. Requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct automated security monitoring and testing, including simulated attacks, penetration tests, and audits on Defendants systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors; protect all data collected through the course of their business in accordance with all applicable regulations,

industry standards, and federal, state or local laws;

iii. Requiring Defendants to delete, destroy and purge the PII of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

v. Requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' networks is compromised, hackers cannot gain access to other portions of Defendants' systems;

vi. Requiring Defendants to conduct regular database scanning and securing checks;

vii. Requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

viii. Requiring Defendants to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

ix. Requiring Defendants to implement a system of testing to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs and systems for protecting PII;

x. Requiring Defendants to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xi. Requiring Defendants to meaningfully educate all Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves;

xii. Requiring Defendants to implement logging and monitoring

programs sufficient to track traffic to and from Samsung servers;

xiii. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment; and

xiv. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein.

c. For an order requiring Defendants to pay for credit monitoring services for Plaintiff and the Class of a duration to be determined at trial;

d. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

e. For an award of punitive damages, as allowable by law;

f. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

g. Pre- and post-judgment interest on any amounts awarded; and

h. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: June 13, 2024

ROSSBACH LAW, P.C.

/s/ William A. Rossbach
William A. Rossbach
401 North Washington Street
P.O. Box 8988
Missoula, MT 59807-8988
Phone: (406) 543-5156
Fax: (406) 728-8878
Email: bill@rossbachlaw.com

CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson, Esq. (PHV Forthcoming)
Yana Hart, Esq. (PHV Forthcoming)
Tiara Avaness, Esq. (PHV Forthcoming)
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
rclarkson@clarksonlawfirm.com
yhart@clarksonlawfirm.com
tavaness@clarksonlawfirm.com

Attorneys for Plaintiff and the Proposed Classes